

ISSN: 0719 – 0832



Serie Bibliotecología y Gestión de Información N° 79, Febrero 2013

**UTEM**

**¿Permite el derecho de acceso a la información pública, el acceso a datos personales?**

**Alfredo Steinmeyer Espinosa**



**D · G · I**

Departamento  
de Gestión de  
Información  
Escuela de  
Bibliotecología

Serie Bibliotecología y Gestión de Información es publicada desde Octubre de 2005 por el Departamento de Gestión de Información de la Universidad Tecnológica Metropolitana. Dr. Hernán Alessandri, 722, 6° piso, Providencia, Santiago, Chile, [www.utem.cl](http://www.utem.cl)

Sus artículos están disponibles en versión electrónica en E-prints in Library and Information Science: <http://eprints.rclis.org> y están indizados e integrados en la base de datos “Fuente Académica” de EBSCO Information Services.

Está registrada en el Sistema Regional de Información en Línea para Revistas Científicas de América Latina, El Caribe, España y Portugal (LATINDEX), en Dialnet, portal de difusión de la producción científica hispana y en DOAJ – Directory of Open Access Journals.

Sitio Web: <http://www.bibliotecarios.cl/servicios/serie-bibliotecologia-y-gestion-de-informacion/>

### **Dirección Editorial**

- Héctor Gómez Fuentes, Director Departamento de Gestión de la Información
- Carmen Pérez Ormeño, Directora Escuela de Bibliotecología

### **Editor Jefe**

Héctor Gómez Fuentes

### **Consejo Editorial**

Académicos del Departamento de Gestión de Información

- Mariela Ferrada Cubillos
- Guillermo Toro Araneda

### **Presidenta del Colegio de Bibliotecarios de Chile A. G.**

Gabriela Pradenas Bobadilla

### **Representante Legal**

Luis Pinto Faverio

### **Decano Facultad de Administración y Economía**

Enrique Maturana Lizardi

### **Secretaria del Departamento de Gestión de Información**

Rossana Flores Cuevas

### **Autorizada su reproducción con mención de la fuente.**

LAS IDEAS Y OPINIONES CONTENIDAS EN LOS TRABAJOS Y ARTÍCULOS SON DE RESPONSABILIDAD EXCLUSIVA DE LOS AUTORES Y NO EXPRESAN NECESARIAMENTE EL PUNTO DE VISTA DE LA UNIVERSIDAD TECNOLÓGICA METROPOLITANA

## ¿Permite el derecho de acceso a la información pública, el acceso a datos personales?

Alfredo Steinmeyer Espinosa \*\*

### Resumen

El presente artículo trata sobre el derecho a la protección de datos personales en el derecho comparado, así como los derechos y principios que lo caracterizan y distinguen del derecho a la vida privada. Analiza la situación actual de este derecho en Chile, particularmente su aplicación en la Administración del Estado. A continuación, se hace una descripción del objeto del derecho de acceso a la información y su relación con el objeto del derecho de acceso o *habeas data* contenido en la Ley N° 19.628, efectuando un análisis acerca del rol encomendado al Consejo para la Transparencia como órgano encargado de velar por la protección de datos personales en la Administración del Estado, relevando algunos problemas que implica utilizar el derecho de acceso a la información pública para acceder a datos personales.

**Palabras claves:** informativa, libertad de información, habeas data

---

\*\* Licenciado en Ciencias Jurídicas y Sociales de la Universidad Adolfo Ibáñez, abogado, chileno, Diplomado en Probidad y Buen Gobierno por la Pontificia Universidad Católica de Chile. Asesor jurídico de la Subsecretaría de Transportes. [asteinmeyere@gmail.com](mailto:asteinmeyere@gmail.com)

**Abstract:**

This paper analyzes the data protection right in the comparative law, their rights and principles which distinguish from the right to privacy. Also analyzes the current situation of this right in Chile and its application in the public sector. Then, describes the freedom of information object and its relation with the *habeas data* right contained in the Law Nr. 19.628, analyzing the function given to the Transparency Council like a Service which guarantee the personal data in the Government, highlighting some issues that represent the use of freedom of information right to access to personal data.

**Keywords:** Privacy law; Freedom of information; habeas data

## INTRODUCCION

Por momentos la protección de datos adquiere relevancia en nuestro país para luego diluirse y solo volver a aparecer cuando surge algún hecho destacado que ponga el tema nuevamente en la discusión o cuando desde la perspectiva económica se constata que Chile no es un lugar seguro para el tratamiento de datos personales. Desde la publicación en 1999 de la Ley N° 19.628, sobre Protección de Datos Personales (en adelante LPDP), no han habido avances sustantivos en la materia y Chile se aleja más de tener un nivel adecuado en el tratamiento de esta clase de datos. Son numerosos los proyectos de ley que se han presentado sobre el tema pero parece no existir el impulso suficiente para que éstos avancen y provoquen los cambios deseados<sup>1</sup>.

Con todo, si bien desde la perspectiva normativa no han habido avances, sí han habido progresos desde el punto de vista doctrinario y jurisprudencial. La Ley N° 20.285, sobre Transparencia y Acceso a la Información, que creó al Consejo para la Transparencia (en adelante CPLT) como una corporación autónoma de derecho público encargada de garantizar el derecho de acceso a la información pública, le encomendó a ese Servicio, entre otras funciones, la de velar por el adecuado cumplimiento de la Ley N° 19.628 por parte de la Administración del Estado<sup>2</sup>.

En ejercicio de esa función residual<sup>3</sup>, ejercida principalmente a través de su función de resolver los amparos que se le presenten por denegación al derecho de

---

<sup>1</sup> En efecto, se han presentado alrededor de 32 proyectos de ley relacionados, de los cuales solo 3 han sido publicados. El más importante es el iniciado por Mensaje (boletín N° 8143-03) e ingresado el 11 de enero de 2012 a la Cámara de Diputados y que actualmente se encuentra en primer trámite constitucional en la Comisión de Economía, Fomento y Desarrollo. Se trata de un proyecto que busca que Chile cumpla con las exigencias establecidas como país miembro de la OCDE; transformarlo en un país con un nivel adecuado de protección y favorecer el desarrollo del mercado de los servicios globales. Establece que es el Consejo para la Transparencia el órgano encargado de resolver los reclamos que se presenten en contra de servicios públicos en tanto que deja en el juez de letras en lo civil la resolución de los reclamos formulados en contra de una entidad privada.

<sup>2</sup> El literal m) del art. 33 de la Ley de Transparencia le ha encomendado al CPLT la función de "velar por el adecuado cumplimiento de la ley N° 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado"

<sup>3</sup> El art. 32 de la Ley de Transparencia señala "*El Consejo tiene por objeto promover la transparencia de la función pública, fiscalizar el cumplimiento de las normas sobre transparencia y publicidad de la información de los órganos de la Administración del Estado, y garantizar el derecho de acceso a la información*" Seguidamente, en su art. 33 señala las funciones atribuciones que le corresponden para dar sustento a esa función principal consistente en garantizar el derecho de acceso a la información. Entre éstas, el CPLT puede dictar instrucciones generales para dar cumplimiento a la legislación sobre transparencia y acceso a la información; formular recomendaciones a los órganos de la Administración del Estado tendientes a perfeccionar la transparencia de su gestión y a facilitar el acceso a la información que posean, y resolver, fundadamente, los reclamos por denegación de acceso a la información que le sean formulados. No obstante, el literal m) del referido art. 33 le entrega una función diversa y que en principio parece no conversar con el resto de las funciones encomendadas. De ahí que se le denomine "residual".

acceso a la información pública, el Consejo ha tenido la oportunidad de revitalizar la discusión sobre la protección de datos personales y los principios que la rigen, incorporando los conceptos e ideas que lo relevan como un derecho de importancia.

Esta función también ha despertado críticas sobre si es el CPLT, el órgano encargado de garantizar el derecho de acceso a la información, el mismo que debería velar por la protección de datos personales<sup>4</sup>. Esa discusión no es el objeto de este trabajo pero se dirá que hay buenas razones para concentrar ambas funciones en un mismo órgano como también hay razonables fundamentos por los cuales es mejor separarlas. Lo cierto es que en el derecho comparado no hay un solo modelo, existiendo casos en que un mismo órgano está encargado de velar por el derecho de acceso a la información y por la protección de datos personales, como casos en que estas funciones se encomiendan a órganos independientes entre sí.<sup>56</sup>

Sin embargo, el CPLT no tiene hoy las facultades para poder ejercer esa función de manera de constituirse como el órgano de control en materia de protección de datos en el sector público. Para ello se requieren modificaciones legales. Ante la falta de atribuciones expresas y dada la ausencia de un órgano de control, el CPLT ha sostenido que a través del derecho de acceso a la información las personas pueden acceder a sus datos personales. Esta interpretación si bien abre a las personas una vía expedita para acceder a sus datos personales, no explica por qué una misma información puede ser “pública” para algunos y reservada para otros, considerando que el objeto del derecho de acceso a la información es información pública.

---

<sup>4</sup> En efecto, se puede ver sobre esto la columna de opinión publicada por el Sr. Renato Jijena en el Diario la Tercera: [http://www.latercera.com/contenido/895\\_146299\\_9.shtml](http://www.latercera.com/contenido/895_146299_9.shtml)

<sup>5</sup> Los ejemplos de comisiones que concentran ambas funciones en un solo órgano son: La Oficina del Comisionado de Información (ICO), de Reino Unido; el Comisionado Federal de Protección de Datos y Libertad de Información, de Alemania y la Oficina del Comisionado de Privacidad de Canadá. Recientemente también el Instituto Federal de Acceso a la Información (IFAI) de México. Por el contrario, la Agencia Española de Protección de Datos, en España; el Garante para la Protección de Datos, en Italia; La Unidad Reguladora y de Control de Datos Personales (URCDP), en Uruguay; y Comisión Nacional de Datos Informatizados (CNDI), en Portugal, atribuyen la defensa de este derecho a un órgano. Fuente: Informe Final “*Diseño de un Modelo Organizacional del Consejo para la Transparencia en su nueva función de Protección de Datos Personales*” Universidad de Chile y el Centro de Sistemas Públicos.

<sup>6</sup> Para quienes defienden que el CPLT asuma esta función en Chile esgrimen que la transparencia y la protección de datos son dos caras de una misma moneda.

En este artículo se hará un breve análisis sobre derecho a la protección de datos personales, su reconocimiento como un derecho fundamental en la legislación comparada y los principios y derechos que lo componen, especialmente el derecho de acceso o *habeas data*. Asimismo, se hará una descripción del objeto del derecho de acceso a la información, su relación con el objeto del derecho de acceso o *habeas data*, y se plantearán algunos problemas que supone acceder a los datos en la Administración a través del derecho de acceso a la información.

## 1) La protección de datos personales como derecho

Ante el desarrollo de herramientas informáticas y de las tecnologías de información en la década de los 70, surgió la necesidad de regular el almacenamiento, procesamiento y destino de los datos personales, los cuales no siempre se encontraban cubiertos por el derecho a la vida privada. El derecho a la protección de datos personales, en efecto, tiene un objeto diverso que el derecho a la intimidad o vida privada, cuyo ámbito de acción está restringido a proteger manifestaciones privadas de la personalidad tales como el domicilio, la correspondencia, la familia, la honra o la reputación<sup>7</sup>. El derecho a la protección de datos personales, en cambio, atribuye al titular de los mismos las facultades y herramientas de control sobre toda clase de datos personales, con independencia de su naturaleza íntima, de si son o no trascendentes e incluso con independencia de su naturaleza pública o privada<sup>8</sup>.

### a) El tratamiento del DPDP en el derecho comparado:

El derecho a la protección de datos personales es tratado en la doctrina y jurisprudencia comparada como un derecho de carácter fundamental<sup>9</sup>. Esta calidad se comenzó a gestar en las constituciones de los años 70, especialmente en la española, alemana y la portuguesa, donde se reconocía tímidamente un derecho a controlar el uso de la información

---

<sup>7</sup> Véase sobre esto Graciela Romero Silvera "Interés Público y Protección de Datos Personales, con especial referencia a los Derechos Humanos; en Seminario Regional de Protección de Datos Montevideo, Uruguay, 2010, P. 6 y 7.

<sup>8</sup> El aspecto positivo del derecho a la vida privada se articula sobre la idea de control, mientras el aspecto negativo lo hace sobre la idea de exclusión. Por eso algunos autores distinguen entre derecho a la vida privada física y derecho a la vida privada informativa. Mediante el primero, se protege la libertad frente a toda intromisión sobre uno mismo, su casa, su familia o relaciones. Mediante el derecho a la vida privada informativa, se determina por cada sujeto cómo y en qué medida se puede comunicar a otros, información sobre uno mismo. En este último sentido, implica la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida. Tomado del Proyecto de Ley sobre protección de datos personales, Boletín N° 6120-08, ingresado a la Cámara de Diputados en octubre de 2008; Pablo Murillo Lucas; "La protección de los datos personales ante el uso de la informática" en Estudios en homenaje al profesor don Luis Sánchez Agesta, Revista Facultad de Derecho, Universidad Complutense (RFDUC), Madrid, 1989. p. 605-606.

<sup>9</sup> Véase sobre esto Ricard Martínez Martínez "El derecho fundamental a la protección de datos: perspectivas", 2007, En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. Revista de Internet, Derecho y Política. N.º 5. UOC. <http://www.uoc.edu/idp/5/dt/esp/martinez.pdf>



personal<sup>10</sup>. Se trata de la primera generación de legislaciones sobre protección de datos personales, que contemplaba el establecimiento de principios de publicidad sobre la existencia de bases de datos; la existencia de autoridades garantes de este derecho, y su aplicación tanto al ámbito público como al ámbito privado<sup>11</sup>. No obstante, no es sino hasta la dictación del Convenio N° 108, del Consejo de Europa, en 1981, que se definen los principios y los derechos que dan forma al derecho a la protección de datos personales tal como lo conocemos en nuestros días. Es en este Convenio donde, además, se urde el concepto de datos sensibles y se establece un modelo de tutela administrativa encomendada a autoridades autónomas.

Es así como nacen los principios de calidad de los datos, finalidad, proporcionalidad y reserva o confidencialidad, entre otros; en tanto que se reconocen los denominados derechos ARCO, esto es, acceso, rectificación, cancelación y oposición.

En consecuencia, la dictación del Convenio N° 108 marca, desde el punto de vista legislativo, el reconocimiento del derecho a la protección de datos personales como un derecho autónomo ligado esencialmente con las tecnologías de información y las comunicaciones, con una estructura, principios y alcance claramente definidos y distinguible del derecho a la intimidad.

Desde el punto de vista jurisprudencial, en tanto, el carácter fundamental del derecho a la protección de datos personales como un derecho a la “autodeterminación informativa” se forja en el seno del Tribunal Constitucional Federal Alemán, en el caso “Ley de Censo de la

---

<sup>10</sup> Véase sobre esto “El Derecho a la Protección de Datos Personales: Historia del derecho a la vida privada y el derecho a la protección de datos” 1ª Edición, 2010, Fundación CEDDET. Pp.19 a 40.

<sup>11</sup> *Ibid.*, p. 23.

Población”<sup>12</sup>. En efecto, el Tribunal reconoció el carácter fundamental de este derecho al señalar que *la protección del individuo en contra la recogida, almacenamiento, utilización y difusión ilimitada de sus datos personales queda englobada en el derecho general de la protección de la persona del artículo 2º, párrafo 1º, de la Ley Fundamental. El derecho constitucional garantiza en esta medida la facultad del individuo de determinar fundamentalmente por sí mismo la divulgación y la utilización de datos referentes a su persona.*

El Tribunal Constitucional Español, a su vez, en la sentencia recaída en la causa rol 292/2000<sup>13</sup>, subrayó la independencia de este derecho respecto del derecho a la intimidad, indicando que *La garantía de la vida privada de la persona y de su reputación poseen una dimensión positiva que exceden el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativo a la propia persona. La llamada libertad informativa es así un derecho a controlar el uso de los mismos datos insertos en un programa informático (...) Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE (...) atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la ley. Agrega el Tribunal que el derecho a la protección de datos personales alcanza a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual (...) sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que*

---

<sup>12</sup> Tomada de: Schwabe, Jürgen (Compilador), Cincuenta Años de Jurisprudencia del Tribunal Constitucional Federal Alemán, Medellín, Colombia, Ediciones Jurídicas Gustavo Ibáñez, Konrad Adenauer Stiftung, Traducción de las sentencias de Marcela Anzola Gil, 2003, pp. 36 a 44.

<sup>13</sup> <http://hj.tribunalconstitucional.es/HJ/es/Resolucion/Show/4276>

*por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan del poder de disposición del afectado*

En suma, el derecho a la protección de datos personales tanto del punto de vista legislativo como jurisprudencial o doctrinario, ha sido reconocido, primero, como un derecho de rango fundamental diverso del derecho a la intimidad y, segundo, con un objeto, mecanismos de tutela y formas de ejercicio particulares, forjado en la idea del control sobre los datos propios, sin embargo de la importancia que éstos pudieren tener.

## **b) Los derechos ARCO.**

Un reflejo del reconocimiento del derecho a la protección de datos como un derecho fundamental diverso del derecho a la intimidad, se explica en la creación de mecanismos específicos de tutela que se traducen en el poder de control que tiene o debe tener el titular sobre sus datos personales. Estos mecanismos, esenciales del derecho a la protección de datos personales, son los denominados derechos ARCO que, como ya se ha dicho, surgen con la dictación del Convenio N° 108, de 1981, y se consolidan con la jurisprudencia de los tribunales constitucionales alemán y español.

Si bien no es el objeto de este trabajo explicar en qué consisten cada uno de estos derechos, se hará un breve repaso sobre el significado y alcance del derecho de acceso o habeas data y el derecho de oposición, habida cuenta de su intrínseca relación con el derecho de acceso a la información pública y con la causal de reserva establecida en el art. 21 N° 2<sup>14</sup> de la LT y el derecho de oposición establecido en el art. 20 del mismo cuerpo legal<sup>15</sup>.

---

<sup>14</sup> Artículo 21 de la Ley de Transparencia: *Las únicas causales de secreto o reserva en cuya virtud se podrá denegar total o parcialmente el acceso a la información, son las siguientes:*

N° 2, *Cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de su seguridad, su salud, la esfera de su vida privada o derechos de carácter comercial o económico (énfasis agregado)*

El derecho de acceso, o habeas data, se ha definido como el derecho que detenta el titular de los datos personales para solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén realizar<sup>16</sup>. El derecho de acceso, por tanto, es la herramienta que impulsa al derecho a la protección de datos personales. Éste requiere, como condición previa para su tutela, la posibilidad de conocer qué datos ligados a una determinada persona tiene el responsable o encargado del tratamiento y con qué finalidad los está tratando.

En el caso español, en el art. 15 de su Ley Orgánica N° 15, de 1999, sobre Protección de Datos Personales, el derecho de acceso se regula definiendo en qué consiste el mismo, cómo puede ejercerse y el lapso de tiempo en que puede lícitamente ejercerse. La legislación española ha procurado que en las formas de consulta se respete el principio de neutralidad tecnológica, considerando que el campo de éstas es dinámico y que, consecuentemente, las formas de ejercicio de este derecho no pueden quedar limitadas según los mecanismos tecnológicos que existan en un determinado momento.

---

<sup>15</sup> Artículo 20 de la Ley de Transparencia: *Cuando la solicitud de acceso se refiera a documentos o antecedentes que contengan información que pueda afectar los derechos de terceros, la autoridad o jefatura o jefe superior del órgano o servicio de la Administración del Estado, requerido, dentro del plazo de dos días hábiles, contado desde la recepción de la solicitud que cumpla con los requisitos, deberá comunicar mediante carta certificada, a la o las personas a que se refiere o afecta la información correspondiente, la facultad que les asiste para oponerse a la entrega de los documentos solicitados, adjuntando copia del requerimiento respectivo.*

*Los terceros afectados podrán ejercer su derecho de oposición dentro del plazo de tres días hábiles contado desde la fecha de notificación. La oposición deberá presentarse por escrito y requerirá expresión de causa.*

*Deducida la oposición en tiempo y forma, el órgano requerido quedará impedido de proporcionar la documentación o antecedentes solicitados, salvo resolución en contrario del Consejo, dictada conforme al procedimiento que establece esta ley.*

*En caso de no deducirse la oposición, se entenderá que el tercero afectado accede a la publicidad de dicha información.*

<sup>16</sup> Fundación CEDDET. Op. Cit., Pp.68 a 90.

En nuestra legislación, la LPDP regula el derecho de acceso en su art. 12, señalando que *“toda persona tiene derecho a exigir a quien sea responsable de un banco, que se dedique en forma pública o privada al tratamiento de datos personales, información sobre los datos relativos a su persona, su procedencia y destinatario, el propósito del almacenamiento y la individualización de las personas u organismos a los cuales sus datos son transmitidos regularmente”* Nuestro ordenamiento jurídico no establece un procedimiento específico para ejercer el derecho de acceso ni tampoco establece un período de tiempo dentro del cual puede ejercerse válidamente.

El derecho de oposición, por su parte, se ha definido como el derecho del interesado a negarse, por motivo legítimos, a que sus datos personales sean objeto de tratamiento o, en caso que los mismos ya estén siendo tratados, a que cese dicha actividad<sup>17</sup>.

En la legislación española este derecho está regulado en el art. 17 de la Ley Orgánica N° 15/1999, no obstante el procedimiento específico se encuentra establecido en el reglamento aprobado por el Real Decreto N° 1820, de 2007, específicamente en su art. 25. En lo que interesa, tanto para el ejercicio del derecho de oposición, como el de acceso, cancelación y rectificación, debe disponerse de un medio sencillo, expedito y gratuito.

En nuestro país el derecho de oposición no está expresamente contemplado. Sí lo están los derechos de “eliminación” y de “modificación” que tienen similitudes con los derechos de cancelación y rectificación pero que, en definitiva, no son lo mismo. En efecto, el derecho de eliminación que contempla nuestra legislación sólo procede en caso que el tratamiento del dato personal carezca de fundamento legal o bien cuando el dato esté caduco. No establece la posibilidad de oponerse *ex ante* al tratamiento de

---

<sup>17</sup> Fundación CEDDET. Op. Cit., p.87.

un dato, como sí lo contempla el derecho de oposición. Además, para ejercer este último bastan motivos “legítimos” en tanto que para requerir la eliminación de dato se requiere que su tratamiento sea ilegal. Con todo, tanto la eliminación como la oposición pueden ejercerse cuando el dato esté caduco.

### c) Principios del derecho a la protección de datos personales.

Otra manifestación del derecho a la protección de datos como un derecho autónomo son los principios que lo rigen. Éstos le dan forma y fijan su sentido y alcance. Así como el derecho de acceso a la información pública se sustenta en principios tales como el de apertura o transparencia, máxima divulgación y no discriminación. El derecho a la protección de datos personales se basa en la idea de calidad de los datos que, a su vez, se sustenta en los principios de licitud, proporcionalidad, veracidad y finalidad.

El principio de licitud implica que el tratamiento de los datos personales debe ser legítimo y legal. En nuestra legislación este principio está contenido en el art. 4 de la ya mencionada Ley N° 19.628, que señala que *“El tratamiento de los datos personales sólo puede efectuarse cuando esta ley u otras disposiciones legales lo autoricen o el titular consienta expresamente en ello”*<sup>18</sup>

Por su parte, el principio de proporcionalidad impone sobre el responsable del tratamiento la obligación de tratar datos que sean adecuados, pertinentes y no excesivos para los fines lícitos para los cuales hayan sido recolectados. El dato personal es en sí mismo un dato protegido y, como tal, debe ser tratado en su justa medida y sólo para los fines para los cuales haya sido recolectado. Es decir, si para un mismo fin es posible recolectar

<sup>18</sup> Cabe señalar que ni aun cuando el titular consienta el tratamiento, si éste no es legítimo o legal, entonces el tratamiento- no obstante el consentimiento- seguirá siendo ilícito.

datos menos invasivos, entonces deben recolectarse esos datos y no otros. En este sentido, el principio de proporcionalidad está intrínsecamente ligado con el principio de finalidad. Éste consiste en que los datos recolectados sólo pueden ser tratados para fines determinados, los cuales deben ser explícitos y legítimos, y sólo para esos fines. Nuestra legislación reconoce este principio en el art. 9° de la Ley N° 19.628, que señala los datos personales deben utilizarse solo para los fines para los cuales hubieren sido recolectados.

Por último, el principio de veracidad implica que los datos tratados sean exactos y representen, en todo momento, el estado actual de su titular. En el citado art. 9° de la Ley N° 19.628, se reconoce este principio al señalar que los datos personales deben ser exactos, actualizados y responder con veracidad a la situación real de su titular.

## **2) El derecho a la protección de datos en Chile.**

El estado del tratamiento de datos personales en nuestro país dista bastante de las exigencias establecidas en legislaciones comparadas, incluso las de nuestra región como Uruguay, México y Argentina<sup>19</sup>. Si bien Chile fue el precursor de una legislación orgánica sobre protección de datos personales, la Ley N° 19.628, de 1999 (mismo año en que se dicta la Ley Orgánica de Protección de Datos de España), aquél cuerpo normativo no recoge algunos principios básicos de este derecho, como el de proporcionalidad, ni contempla- como se ha dicho- la posibilidad de ejercer el derecho de oposición. Adicionalmente, nuestra legislación no contempla una acción específica y expedita para tutelar

---

<sup>19</sup> En efecto, Argentina cuenta con la Dirección Nacional de Protección de Datos Personales, como un órgano descentralizado del Ministerio de Justicia y Derechos Humanos de la Nación, con autonomía funcional y dirigido por un Director elegido por el Ejecutivo con concurso de oposición para un período de cuatro años (artículo 29 de la Ley 25.326); En Uruguay existe la Unidad Reguladora y de Control de Datos Personales (URCDP) creada por la Ley N° 18.331 de Protección de Datos Personales y Acción de Habeas Data (LPDP), con autonomía técnica, cuya competencia es custodiar el cumplimiento de la legislación de protección de datos personales y asegurar el respeto de sus principios y en México existe el Instituto Federal de Acceso a la Información y Privacidad, creado por la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

el derecho a la protección de datos personales ni cuenta con una autoridad administrativa encargada de garantizar este derecho<sup>20</sup>.

En este sentido, es importante recordar que la protección de datos personales se funda en el principio de la autodeterminación informativa, que significa que el titular de un dato de carácter personal tiene derecho a conocer, acceder, rectificar, cancelar y controlar las informaciones concernientes a sí mismo<sup>21</sup>. Este principio no lo recoge nuestro ordenamiento jurídico toda vez que no consagra expresamente el derecho de las personas a controlar sus datos. En su lugar, la LPDP se limita a establecer el derecho a efectuar el tratamiento de datos personales, con referencia a que tal tratamiento debe respetar los derechos de los titulares. Asimismo, parte de la base de que la información objeto de tratamiento es pública y que, por tanto, no requiere de la autorización de sus titulares para procesarse.

Por lo tanto, si bien nuestro país cuenta con una legislación específica sobre protección de datos personales ésta no ha sido construida sobre la base del control que deben tener los titulares sobre esos datos- elemento de la esencia de este derecho- sino sobre la libertad en el tratamiento de los mismos.

En cualquier caso, la LPDP establece el derecho de acceso, además de los derechos de eliminación y modificación, los cuales deben ejercerse por parte del titular de los datos ante el responsable de tratamiento. Para el supuesto en que el responsable del tratamiento no de respuesta al interesado o bien deniegue la información por causas distintas al interés nacional o la seguridad de la Nación, la ley dispone en su artículo 16 un procedimiento de amparo ante una autoridad judicial. En efecto, señala el referido art., que *“el titular de los*

---

<sup>20</sup> Sin perjuicio de lo que se dirá sobre el Consejo para la Transparencia.

<sup>21</sup> Véase sobre esto Isabel-Cecilia del Castillo V. Protección de datos: *“Cuestiones constitucionales y administrativas”*. Madrid: Thomson-Civitas, 2007, pp. 213-241.



datos tendrá derecho a recurrir al juez de letras en lo civil del domicilio del responsable”<sup>22</sup>

**a) La jurisprudencia del Tribunal Constitucional en materia de protección de datos.**

Si bien ya en 1999 la recién publicada Ley 19.628 reconocía- con las debilidades que se han observado- el derecho a la protección de datos personales, a la jurisprudencia emanada del Tribunal Constitucional (TC) le llevó más tiempo diferenciar ese derecho del derecho a la vida privada. En efecto, la primera jurisprudencia del Tribunal Constitucional sobre la materia, contenida en las sentencias de 4 de enero de 1995<sup>23</sup>; de 28 de octubre de 2003<sup>24</sup>, y luego en la sentencia de 8 de abril<sup>25</sup> de 2010<sup>26</sup>, no aparece una diferenciación entre el derecho a la protección de datos personales de la garantía constitucional contenida en el art. 19 N° 4 de la Constitución Política de la República, a pesar de tratarse de casos en que se configuraban los supuestos necesarios para pronunciarse sobre el derecho a la protección de datos personales como un derecho autónomo. Especialmente en el último caso mencionado, en que el TC se pronunció sobre la constitucionalidad en la toma de muestras biológicas de forma forzada a una persona condenada para extraer su huella genética e incorporarla al Sistema Nacional de Registros de ADN. Allí el TC señaló que *Puede afirmarse, entonces, que la privacidad de las personas condenadas, que se encuentran en los supuestos descritos por la ley nro. 19.970, se ve afectada, en forma precisa y determinada, y sólo en la medida que dicha afectación coadyuve al*

<sup>22</sup> Sobre esto, el autor Alberto Cerda Silva ha dicho: *No se trata, contrariamente a lo que se pudiera pensar, de una absoluta prescindencia estatal en relación con los problemas propios del tratamiento de los datos personales. De hecho, tanto en un modelo como en el otro los Estados han reglamentado legalmente el tratamiento de tales datos y, por supuesto, siempre es posible recurrir a la autoridad judicial para obtener la resolución de los conflictos suscitados en relación con tal normativa*” “Hacia un modelo integrado de regulación y control en la protección de datos personales”, Santiago, 2008, P. 123.

<sup>23</sup> Rol 198-94

<sup>24</sup> Rol 389-03

<sup>25</sup> Rol 1365-09

<sup>26</sup> Véase sobre esto Flavio Quezada Rodríguez “La protección de datos personales en la jurisprudencia del Tribunal Constitucional de Chile”; Santiago, 2012, Revista Chilena de Derecho y Tecnología. Vol., N° 1, P 125-147.

*cumplimiento de los objetivos que persigue el legislador, según se profundizará más adelante» (considerando veintisiete).*

De esta manera el TC trata el derecho a la privacidad como un derecho negativo, esto es, un derecho a evitar intromisiones de terceros, salvo que esa intromisión sea precisa y determinada, y esté permitida por ley. Este es precisamente el concepto que hay detrás de la protección de datos. Se trata de una libertad positiva donde el titular tiene derecho a controlar sus datos personales.

Sin perjuicio de lo anterior, a través de esta jurisprudencia el TC estableció un principio básico del derecho a la protección de datos personales como lo es la necesidad de contar con el consentimiento del afectado<sup>27</sup>, junto con señalar que el derecho a la privacidad no es absoluto, encontrándose el legislador habilitado para regular su ejercicio, en la medida en que no se afecte el derecho en su esencia.

En una decisión más reciente<sup>28</sup>, en respuesta al requerimiento de inaplicabilidad por inconstitucionalidad del artículo décimo, letra h), de la Ley N° 20.285<sup>29</sup>, que obliga a publicar las remuneraciones anuales de cada Director, Presidente Ejecutivo o Vicepresidente Ejecutivo y Gerentes responsables de la dirección y

<sup>27</sup> Quezada Rodríguez, Flavio Op. Cit., p.132.

<sup>28</sup> Rol 1800-10. Requerimiento de inaplicabilidad por inconstitucionalidad presentado por Televisión Nacional de Chile "TVN" respecto de los artículos décimo h) y 33 b) de la Ley N° 20.285, en los autos Rol N° 945-2010 sobre reclamo de ilegalidad interpuesto ante la Corte de Apelaciones de Santiago en contra del Consejo para la Transparencia.

<sup>29</sup> Artículo décimo Ley N° 20.285 "El principio de la transparencia de la función pública consagrado en el inciso segundo del artículo 8° de la Constitución Política y en los artículos 3° y 4° de la Ley de Transparencia de la Función Pública y Acceso a la Información de la Administración del Estado es aplicable a las empresas públicas creadas por ley y a las empresas del Estado y a las sociedades en que éste tenga participación accionaria superior al 50% o mayoría en el directorio, tales como Televisión Nacional de Chile, la Empresa Nacional de Minería, la Empresa de Ferrocarriles del Estado, la Corporación Nacional del Cobre de Chile o Banco Estado, aun cuando la ley respectiva disponga que es necesario mencionarlas expresamente para quedar sujetas a las regulaciones de otras leyes"

*En virtud de dicho principio, las empresas mencionadas en el inciso anterior deberán mantener a disposición permanente del público, a través de sus sitios electrónicos, los siguientes antecedentes debidamente actualizados:*

*h) Toda remuneración percibida en el año por cada Director, Presidente Ejecutivo o Vicepresidente Ejecutivo y Gerentes responsables de la dirección y administración superior de la empresa, incluso aquellas que provengan de funciones o empleos distintos del ejercicio de su cargo que le hayan sido conferidos por la empresa, o por concepto de gastos de representación, viáticos, regalías y, en general, todo otro estipendio. Asimismo, deberá incluirse, de forma global y consolidada, la remuneración total percibida por el personal de la empresa.*

administración superior de empresas públicas, el TC hizo referencia expresa al derecho a la protección de datos personales señalando que (...) *la protección de la vida privada de las personas guarda estrecha relación con la protección de los datos personales, configurando lo que la doctrina llama derecho a la autodeterminación informativa* (considerando vigesimoquinto) Agrega que el derecho a la autodeterminación informativa *se traduce en el control de las personas sobre sus datos y comprende el derecho a saber sobre la existencia de ficheros a archivos de registro de información de carácter personal, públicos o privados, cuáles son sus finalidades y quiénes son los responsables de los mismos, de manera que las personas concernidas puedan conocer los datos propios contenidos en dichos archivos o ficheros, teniendo derecho a actualizarlos o solicitar mediante el recurso de habeas data su rectificación o cancelación”*

Si bien el TC en este caso reconoce y diferencia el derecho a la protección de datos personales del derecho a la privacidad, destacando el elemento esencial del primero como lo es el derecho de control sobre los datos de que se sea titular - indicando además que el dato “remuneración” un dato de carácter personal- parece entender que la idea de control solo se justifica en los casos en que esté en juego un dato sensible y termina por centrarse más bien en el derecho a tratar los datos personales que en el legítimo derecho que le asiste a sus titulares a controlarlos.<sup>30</sup>

Nuestro Tribunal Constitucional en sus últimos fallos ha reconocido también la existencia de este derecho, no obstante aún es posible notar algunas inconsistencias relativas a tratarlo como una libertad negativa a pesar de discurrir expresamente sobre la idea de la autodeterminación informativa. Es importante mencionar que el reconocimiento de este derecho no lo eleva per se a rango fundamental. Nuestra Constitución no reconoce el derecho a la

---

<sup>30</sup> Considerando vigesimoséptimo: (...) “La sociedad actual no podría funcionar sin el tratamiento legal de los datos personales, lo que se ve facilitado por la aplicación de la informática.”

protección de datos personales como un derecho fundamental, sin perjuicio que algunas hipótesis de afectación de datos personales puedan subsumirse en la garantía contenida en el art. 19 N° 4 de nuestra Carta Fundamental.

### **3) La protección de datos y el Consejo para la Transparencia.**

#### **a) La recomendación sobre protección de datos personales.**

Nuestra legislación no contempla la existencia de un organismo de control administrativo y de carácter autónomo que garantice el efectivo ejercicio del derecho a la protección de datos personales. No obstante, la LT en el literal m) de su art. 33 ha encomendado al Consejo para la Transparencia la función de velar por el adecuado cumplimiento de la LPDP por parte de los órganos de la Administración del Estado. Esta función, si bien carente de atribuciones expresas, conversa con otra de sus atribuciones consistente en velar por la debida reserva de los datos e informaciones que conforme a la Constitución y a la ley tengan carácter secreto o reservado, contenida en el literal j) del referido artículo.

En ejercicio de estas funciones y utilizando su atribución consistente en formular recomendaciones a los órganos de la Administración del Estado tendientes a perfeccionar la transparencia de su gestión y a facilitar el acceso a la información que posean, el Consejo dictó en el año 2011 una recomendación sobre protección de datos personales dirigida a la Administración del Estado.

En la recomendación aparece un esfuerzo por sistematizar los conceptos, principios y derechos establecidos, a veces no en forma evidente, en la LPDP y complementarlos con algunas ideas y elementos básicos contenidos en la doctrina y jurisprudencia sobre protección de datos. De

este modo, la recomendación aborda, además de los principios que ya se han comentado, los principios de confidencialidad o secreto y de información. Asimismo, delimita el alcance del derecho de acceso a los datos propios y describe algunas obligaciones específicas que pesan sobre los órganos de la Administración del Estado, tales como el tratamiento de datos personales relativos a delitos, infracciones administrativas o faltas disciplinarias<sup>31</sup>.

Respecto al principio de confidencialidad o secreto, el CPLT se remite a lo dispuesto en el art. 7° de la LPDP, que señala *las personas que trabajan en el tratamiento de datos personales o tengan acceso a éstos de otra forma (como aquellos funcionarios públicos autorizados para el acceso a bancos de datos de los organismos respectivos), están obligadas a guardar secreto sobre los mismos, cuando provengan o hayan sido recolectados de fuentes no accesibles al público, como asimismo sobre los demás datos y antecedentes relacionados con el banco de datos, obligación que no cesa por haber terminado sus actividades en ese campo.*

Por su parte, en cuanto al principio de información, el Consejo efectúa una sugerencia a la Administración del Estado- la que puede tratar datos sin el consentimiento de titular cuando lo haga dentro del ámbito de su competencia- <sup>32</sup> consistente en que, previo a la recolección de los datos, se informe a su titular acerca de la identidad del órgano responsable de la base de datos, de la finalidad perseguida con el tratamiento de la información, de la posible comunicación a terceros y de los derechos que pueden ser ejercidos por ellos.

---

<sup>31</sup> Véase: [http://www.consejotransparencia.cl/consejo/site/artic/20121026/asocfile/20121026095108/recomendacion\\_pd.pdf](http://www.consejotransparencia.cl/consejo/site/artic/20121026/asocfile/20121026095108/recomendacion_pd.pdf)

<sup>32</sup> Art. 20 Ley N° 19.628: *El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular.*

En cuanto al derecho de acceso los datos propios, el Consejo aborda someramente la disyuntiva que se produce cuando alguien, en ejercicio del derecho de acceso a la información, solicita datos de los cuales es su titular. Para este caso el CPLT estima que el procedimiento a aplicar es el establecido en la Ley de Transparencia, incluyendo la posibilidad de recurrir de amparo ante ese servicio.

## **b) Resolución de amparos y la protección de datos.**

El CPLT en ejercicio de su atribución consistente en resolver los reclamos por denegación al derecho de acceso a la información, se ha visto en la necesidad de ponderar el derecho de acceso a la información con el derecho a la protección de datos personales, efectuando un test de proporcionalidad o de interés público<sup>33</sup>.

En ejecución de esta labor el CPLT ha dado acceso a los titulares de datos personales a la información que les concierne, consolidando la idea del control que aquéllos deben mantener sobre sus datos, y denegando información en otros casos por afectarse el derecho de protección de datos personales de las personas. Resulta relevante señalar que el CPLT ha reconocido expresamente que el bien jurídico protegido por la Ley N° 19.628 es el derecho a la autodeterminación informativa<sup>34</sup>.

<sup>33</sup> Véase Rajevic, Mosler; ENRIQUE. "Protección de datos y transparencia en la administración pública chilena: inevitable y deseable ponderación" Santiago, 2010, pp., 1 a 19.

<sup>34</sup> Resolución Amparo C 833.11: Considerando 9) *Que, siguiendo el razonamiento anterior, este Consejo ha considerado que la divulgación de datos como los solicitados importaría afectar los derechos de las personas en los términos de la causal de reserva contenida en el numeral 2 del artículo 21 de la Ley de Transparencia, particularmente el derecho a la vida privada en su vertiente positiva, esto es, la autodeterminación informativa, entendida como la potestad de controlar la información propia.* Resolución Amparo C901-11, considerando 10) *Que, a mayor abundamiento, la entrega de información en este sede, por aplicación del artículo 19 de la Ley de Transparencia, debe realizarse sin imponer condiciones de uso de la misma o restricciones a su empleo, de modo que, tratándose de datos personales recolectados para un fin determinado por la Universidad, la comunicación de la nómina requerida supondría despojar a sus titulares de los datos que contienen el control de su propia información, lesionándose su autodeterminación informativa, bien jurídico protegido por la Ley N° 19.628.*

Así, por ejemplo, en la resolución del amparo A29-09, el CPLT otorgó a la reclamante el acceso sus evaluaciones psicolaborales en un concurso de alta dirección pública, desechando el argumento planteado por el órgano reclamado en orden a que se configuraría la causal de reserva contenida en el art. 21 N° 2 de la Ley de Transparencia pues el titular de los informes psicolaborales no sería el postulante sino la autoridad que solicitó la asesoría profesional para efectuar dicha evaluación. El Consejo estableció que aunque el informe haya sido encargado por el órgano reclamado, el titular de los datos allí contenidos es la persona a que se refieren dichos datos, en este caso, el postulante requirente, de acuerdo a lo dispuesto en el art. 2° letra ñ) de la Ley N° 19.628.

Por su parte, en la resolución del amparo C901-11, donde se requería la nómina de los alumnos de la carrera de medicina, por semestre, desde el año 2000 (ingreso) hasta el 2008 (egreso), el CPLT denegó su acceso pues estimó que ésta correspondía a información que contiene datos de carácter personal de terceros distintos al reclamante, en los términos dispuestos por el literal f) del artículo 2° de la Ley N° 19.628, sobre Protección de la Vida Privada, toda vez que tal información supone divulgar el nombre, carrera universitaria y casa de estudios de determinadas personas naturales, vale decir, se trata de “información concerniente a personas naturales, identificadas o identificables”.

Nótese que el CPLT no necesitó evaluar si los datos “nombre”; “carrera universitaria y “casa de estudios” eran trascendentes y si con su revelación se afectaba el honor o el derecho a la intimidad de sus titulares. Por el contrario, simplemente evaluó si, por una parte, existía el consentimiento por parte de los titulares para tratar tales datos y, en caso de no existir, si se configuraba la excepción a ese consentimiento consistente en que el

órgano tratase dichos datos en el ámbito de sus competencias. En este sentido el Consejo verificó que no existía el consentimiento de los titulares y que si bien el órgano estaba facultado para tratar aquellos datos, no lo estaba para transferirlos u ocuparlos para fines diversos a los establecidos en la respectiva legislación. De esta forma el CPLT señaló que *la comunicación de la nómina requerida supondría despojar a sus titulares de los datos que contienen **del control de su propia información, lesionándose su autodeterminación informativa, bien jurídico protegido por la Ley N° 19.628***”

#### **4) Datos personales como información en poder del Estado y el derecho de acceso a la información para acceder a datos personales.**

##### **a) Sobre el objeto del derecho a la protección de datos personales y su relación con el objeto del derecho de acceso a la información.**

Si bien mediante el ejercicio del derecho de acceso a la información y el derecho de acceso regulado en el art. 12 de la LPDP se puede, en la práctica, acceder a información, lo cierto es que el objeto, principios y procedimientos de éste y aquél son completamente diversos.

Mientras que el derecho de acceso a la información tiene por objeto acceder a los actos y resoluciones de los órganos de la Administración del Estado, sus fundamentos, los documentos que les sirvan de sustento o complemento directo y esencial, y los procedimientos que se utilicen para su dictación, además de a la información elaborada con presupuesto público y toda otra que obre en poder del Estado<sup>35</sup>, el derecho de acceso o habeas data tiene por objeto acceder a datos personales o a datos sensibles. Mientras que el primero puede ser ejercido por cualquier persona

<sup>35</sup> Sobre esto véase CONTRERAS, Pablo y PAVÓN, Andrés (2012): “La Jurisprudencia del Consejo para la Transparencia sobre Acceso a la Información Pública y Seguridad de la Nación”, en *Ius et Praxis* (Vol. 18, No. 2).



y sin expresión de causa el segundo sólo puede ser ejercido por el titular del dato personal. Mientras que el primero se rige por el principio de máxima divulgación el segundo se rige por el principio de confidencialidad.

Finalmente, mientras que en caso de denegación del derecho de acceso a la información la autoridad llamada a pronunciarse es el CPLT, en caso de denegación del habeas data (o el derecho de cancelación o rectificación) la autoridad competente es el Juzgado de Letras en lo Civil correspondiente.

Otra diferencia importante es el reconocimiento del derecho de acceso a la información como un derecho fundamental, atendido lo dispuesto en el art. 8° en relación con el art. 19 N° 12, ambos de la Constitución Política, cuestión que no ocurre en nuestro ordenamiento jurídico con el derecho a la protección de datos personales. Si bien el CPLT ha “ponderado” el derecho de acceso con el derecho a la protección de datos personales en su decisiones, lo ha hecho por la relación que existe entre éste y la garantía constitucional contenida en el art. 19 N° 4, esto es, el derecho a la protección a la vida privada y a la honra de la persona y su familia, y porque en definitiva el dato personal puede estar contenido en la causal de reserva establecida en el art. 21 N° 2 de la Ley de Transparencia. Pero, de nuevo, no porque el derecho a la protección de datos personales sea un derecho fundamental en nuestro país.

#### **b) El acceso a datos personales a través del derecho de acceso a la información.**

La naturaleza antagónica de ambos derechos surge cuando en una solicitud de información se requiere información que además contiene datos que son de carácter personal, lo que obliga a decidir si prevalece la reserva de los

datos personales o el interés público en dar a conocer la información solicitada, sin perjuicio de aplicar el principio de divisibilidad y el procedimiento establecido en el artículo 20<sup>36</sup> de la Ley de Transparencia. Ahora bien, esta ponderación sólo es necesaria cuando quien pide la información que contiene datos personales no es el titular de esos datos personales. Cuando quien pide la información es a la vez el titular de los datos que se requieren, entonces surge la pregunta de si ocupar el procedimiento de acceso a la información pública resulta plausible.

El CPLT resolvió este tema en su recomendación sobre protección de datos personales señalando que *cuando en el ejercicio del derecho de acceso a la información pública establecido en la Ley de Transparencia, se soliciten antecedentes que, obrando en poder de la Administración, contengan datos personales de los que es titular el solicitante, se aplicará el procedimiento establecido en dicha Ley, incluyendo la posibilidad de recurrir de amparo ante este Consejo. No obstante ello, en lo relativo a la gratuidad del acceso, se observará lo dispuesto en la Ley N° 19.628.*

El Consejo no ha dicho que el titular de un dato personal pueda, a través del procedimiento de acceso a la información, requerir a la Administración del Estado sus datos personales. Lo que ha dicho es que si en el ejercicio del derecho de acceso y requiriendo la información que la Constitución y la Ley han declarado como información pública, ésta contiene además datos personales, entonces se podrá acceder a ellos por esa vía.

Luego, ¿quiere decir esto que si alguien sólo pide un dato personal, por ejemplo, el resultado de una evaluación laboral que se le ha practicado, no podría ocuparse el procedimiento de acceso a la información? La clave está en lo que la Constitución y la Ley han definido como información pública.

---

<sup>36</sup> Se refiere al derecho de oposición.

Ésta incluye actos, resoluciones, documentos y, en fin, cualquier información que obre en poder del Estado. Siendo así, si esa información- la evaluación laboral- está contenida en algún “documento” entonces pasa a ser información en principio pública y es susceptible de ser requerida mediante el derecho de acceso.

No obstante, esto plantea otra disyuntiva: ¿es posible que una misma información- la evaluación laboral- sea pública para el requirente/titular pero reservada para terceros? Si se señala que la información “evaluación laboral” es reservada pues está protegida, digamos, por la causal contenida en el numeral 2 del art. 21 de la Ley de Transparencia y que mediante una ficción legal esa reserva se “levanta” cuando quien la pide es su titular, entonces lo que estamos diciendo es que esa información ya no puede subsumirse en el objeto del derecho de acceso a la información. La información, en esas condiciones, dejó de ser pública y eso aplica a todas las personas incluido el titular (de lo contrario habría que defender que la información “evaluación laboral” es pública pero que terceros a ella no pueden conocerla, lo cual supondría una falacia lógica) De tal manera que si la información es reservada entonces el procedimiento a aplicar no podría ser otro que el establecido en la Ley N° 19.628; si es pública entonces habría que entregarla incluso a quienes no sean sus titulares.

**c) Aplicación de la protección de datos personales a la Administración<sup>37</sup>:  
art. 20 de la Ley N° 19.628 y art. 33 m) y b) de la Ley de Transparencia**

La función encomendada al Consejo respecto de la protección de datos personales está restringida, como se ha dicho, a velar por el debido cumplimiento de la Ley N° 19.628 por parte de los órganos de la Administración del Estado. La obligación que recae sobre éstos, por su

<sup>37</sup> Sobre esto véase Rodrigo Gutiérrez Castro “Consideraciones y Recomendaciones en materia de tratamiento de datos personales por organismos públicos” presentado en seminario técnico “Protección de datos personales”, organizado por Expansiva y la Facultad de Derecho de la Universidad de Chile, realizado el 1 de agosto de 2008.

parte, está definida en el artículo 20 de dicho cuerpo normativo que dispone *El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular*

El consentimiento del titular del dato personal es un elemento de la esencia de los principios que gobiernan el derecho a la autodeterminación informativa y que legitima el tratamiento de los datos de carácter personal. En efecto, para llevar a cabo un determinado tratamiento de datos personales el responsable de tal tratamiento debe informar previamente al titular de esos datos y obtener su consentimiento; entendido este último como la manifestación de la voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de datos personales que le conciernen<sup>38</sup>.

Con todo, nuestra legislación establece algunas excepciones a la regla del consentimiento como ocurre cuando los datos hayan sido recolectados desde una fuente accesible al público o cuando exista una autorización legal que exima de dicho consentimiento. Este último es el supuesto a que se refiere el art. 20 en donde el legislador ha soslayado esa manifestación de la voluntad por la existencia de un interés público superior. No obstante, el tratamiento en esas condiciones, aun cuando no requiere el consentimiento de los afectados, sí deben- en principio- mantenerse en reserva por aplicación de lo dispuesto en el art. 7° de Ley N° 19.628, que obliga a los funcionarios públicos que trabajen en el tratamiento de datos personales a guardar secreto sobre los mismos cuando no hayan sido recolectados desde una fuente accesible al público.

---

<sup>38</sup> Fundación CEDDET. Op. Cit., P. 29.

Mediante la resolución de amparos al derecho de acceso a la información y en uso de las facultades que tiene para dictar recomendaciones generales, el Consejo ha tenido la oportunidad de pronunciarse sobre estas materias. En la mayoría de los casos, sin embargo, se ha concentrado más bien a ponderar la publicidad de los datos personales cuando éstos no han sido recolectados de una fuente accesible al público (y no se cuenta con el consentimiento de sus titulares para revelarlos) que sobre si el Servicio respectivo tenía o no las facultades para tratar datos personales. Sin perjuicio de lo anterior, en la resolución del amparo C901-11, que se comentó anteriormente, el Consejo fue un poco más allá evaluando si se configuraba esta regla excepcional y el servicio estaba tratando datos en el ámbito de su competencia: *Que, con todo, ha de colegirse que, en el presente caso, el almacenamiento de datos personales realizado por la USACH se encuentra autorizado por el citado artículo 20, con el objeto de “otorgar grados académicos y títulos profesionales reconocidos por el Estado”, conforme lo establece el artículo 2º, letra d), del D.F.L. N° 1, de 1980, del Ministerio de Educación, que Fija Normas sobre Universidades, sin que resulte procedente la comunicación de tales datos para fines diversos al consignado, como ocurriría en la especie.*

El Consejo también ha delimitado el alcance de lo dispuesto en el art. 21 la Ley N° 19.628, sobre tratamiento de datos relativos a condenas por delitos, infracciones disciplinarias o faltas administrativas. En efecto, el Consejo señaló en la decisión recaída en el amparo rol N° A16-09, los siguiente: *el SAG debe aplicar el principio de divisibilidad previsto en el artículo 11, literal e), de la Ley de Transparencia, respecto de la información relativa a las infracciones y presuntos delitos, **excluyendo los datos personales relativos a condenas, una vez que haya prescrito la acción penal o administrativa, o esté cumplida o prescrita la sanción o pena, así como el R.U.N. o el R.U.T. y el domicilio de los terceros a los que se refieran, dado que estos últimos datos personales no provienen o ni han sido***

*recolectados de fuentes accesibles al público, debiendo guardar el secreto establecido en el artículo 7° de la Ley N° 19.628.*(Énfasis agregado)

En el mismo orden de ideas, el Consejo estableció en su Recomendación sobre Protección de Datos Personales que por aplicación del referido artículo 21, los órganos deben abstenerse de publicar en los actos y resoluciones que tengan efectos sobre terceros, los datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias una vez prescrita la acción penal o administrativa, o cumplida o prescrita la sanción o la pena, aplicando, de ser procedente, el principio de divisibilidad respecto de los actos o resoluciones que los contengan.

No obstante, el Consejo deja la puerta abierta a declarar eventualmente la publicidad de tales datos personales si conociendo de un amparo al derecho de acceso o un reclamo por incumplimiento de las normas sobre transparencia activa, existiera un interés público preponderante.

**d) El rol del CPLT en materia de protección de datos. ¿Órgano de control?**

De lo expuesto se desprende que la función establecida en el literal m) del art. 33 de la Ley de Transparencia ha sido ejercida por el Consejo principalmente a través de la resolución de amparos al derecho de acceso a la información. Se trata, por tanto, de una función que ejerce “residualmente” a su labor principal, cual es garantizar el derecho de acceso a la información.

El Consejo no tiene atribuciones expresas sobre la materia como para poder convertirse en un órgano de control sobre protección de datos en la Administración del Estado y consecuentemente lo que ha hecho por el

desarrollo de este derecho es loable pero limitado. Loable porque es el único Servicio de la Administración que se ha ocupado del derecho a la protección de datos personales aplicando criterios y principios que van más allá de lo dispuesto en nuestra pretérita legislación; pero limitado porque, además de no tener atribuciones que le den valor a su función de “velar”, su mirada de este derecho se plantea en ocasiones desde la incomodidad. La balanza en la que el CPLT pondera el interés público muchas veces está inclinada hacia el acceso a la información.

También es destacable el esfuerzo que hizo el CPLT al haber dictado la recomendación sobre protección de datos personales. Con todo, aquello lo hizo en forma tímida porque, en rigor, carece de atribuciones para dictar recomendaciones sobre esta disciplina. Y es que si bien el CPLT tiene la facultad de dictar recomendaciones éstas deben versar sobre la transparencia en la gestión de los órganos de la Administración y no sobre protección de datos personales.

## Conclusión

Si se trata de generar cambios en el estado de la protección de datos en Chile y, por sobre todo, crear mecanismos de tutela expeditos, lo cierto es que se requieren modificaciones legales e incluso constitucionales. Entre esas modificaciones se requiere la creación de un órgano administrativo autónomo capaz de fiscalizar el cumplimiento del derecho a la protección de datos personales y de resolver los reclamos que se presenten por la ciudadanía ante el tratamiento indebido de sus datos. Ello puede ocurrir otorgándole atribuciones expresas al CPLT que le permitan convertirse en el órgano de control sobre protección de datos o creando un órgano administrativo independiente cuyo objeto sea garantizar este derecho<sup>39 40</sup>.

Mientras ello no ocurra el derecho a la protección de datos seguirá existiendo bajo el alero del derecho a la vida privada, relegando los principios y derechos que lo distinguen de éste a pronunciamientos frágiles y procedimientos ambiguos.

---

<sup>39</sup> En el proyecto de ley, boletín 6120-07, iniciado por mensaje en octubre de 2008, se le entregan amplias facultades al CPLT. Entre éstas, mantener un Registro Único Nacional de las Bases de Datos; fiscalizar el cumplimiento de las disposiciones sobre tratamiento de datos personales, pudiendo recabar, en cualquier momento, del responsable del respectivo registro o banco de datos, la información que estime pertinente; inspeccionar los registros o bancos de datos personales a efectos de verificar el cumplimiento de las obligaciones que establece la ley; requerir la inscripción de los bancos de datos, que no estén registrados, en el Registro Único Nacional; dictar instrucciones de carácter general o particular, respecto de las condiciones de legitimidad de un tratamiento de datos; conocer de las reclamaciones de particulares relacionadas con el ejercicio de sus derechos, señalados en la ley N° 19.628 y en otras normas sobre protección de datos personales, sin perjuicio de las facultades de otras autoridades públicas. Asimismo, se le entregan potestades sancionadoras; requerir a los responsables y encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta ley y, en su caso, ordenar la cesación de los tratamientos y cancelación del registro, cuando no se ajuste a sus disposiciones; ejercer facultades en beneficio directo de las personas. En este sentido, podrá proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal y promover el respeto de los mismos; ejercer el control y adoptar las autorizaciones que procedan para las transferencias internacionales de datos, conforme lo establecido en la ley N° 19628; así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

<sup>40</sup> Por su parte, en el proyecto de ley boletín 8143-03, iniciado por mensaje en enero de 2012, también se le entregan atribuciones al CPLT pero sólo respecto a las reclamaciones que se presenten en contra de Servicios Públicos. (Artículo 16 A.- Procedimiento de reclamo en contra de un organismo público. *En caso que el requerido sea un organismo público definido en el inciso primero de la letra k) del artículo 2° de esta ley, el titular podrá reclamar de las infracciones cometidas ante el Consejo para la Transparencia, en los términos establecidos en los artículos 24, 25 y 27 de la Ley N° 20.285 que resolverá el reclamo y, en su caso, podrá determinar la sanción aplicable al organismo y las responsabilidades administrativas de sus funcionarios, de acuerdo a la facultad dispuesta en la letra m) del artículo 33 de la Ley 20.285*)

En cambio, las reclamaciones que se presenten en el sector privado deberán ser atendidas por el juez de letras en lo civil, no obstante se le entregan algunas atribuciones al Servicio Nacional del Consumidor.



El CPLT ha hecho una valiosa tarea como órgano encargado de garantizar el derecho de acceso a la información pública, y realizado un esfuerzo meritorio al tomarse en serio su rol de velar por la protección de datos personales en el sector público, a pesar de no tener atribuciones expresas sobre el tema. El CPLT ha querido adoptar un rol protagónico sobre la protección de datos desde donde mejor lo hace: resolviendo amparos al derecho de acceso a la información. Desde ahí ha podido pronunciarse, entre otros, sobre los principios de finalidad y proporcionalidad; aplicar el test de interés público o test de daño<sup>41</sup>; reconocer el acceso a datos personales por parte de sus titulares y denegarlos a terceros cuando pueda configurarse la causal de reserva del art. 21 N° 2 de la Ley de Transparencia.

Pero este esfuerzo tiene fragilidades que no pueden soslayarse. Los datos personales que obren en poder del Estado son en principio información reservada y, por lo tanto, no podría accederse a ellos a través del procedimiento de acceso a la información pública, ni aun por sus titulares<sup>42</sup>. El objeto del derecho de acceso a la información es información pública, no reservada. El procedimiento para acceder a los datos personales está contenida en la Ley N° 19.628, y el pronunciamiento en caso de denegación está encomendado a los tribunales de

---

<sup>41</sup> Sobre esto el CPLT señaló en la resolución del amparo C315-11, (considerando 5°) “Que, sin embargo, no toda información subsumible en la categoría de dato personal es per se secreta, pues ello obviaría la inteligencia o sentido de la regla de publicidad de la información que obre en poder de la Administración del Estado, contenida en los artículos 5°, 11 letra c) y 21 de la Ley de Transparencia. Para abordar esta problemática este Consejo ha optado por circunscribir los efectos de sus decisiones al caso concreto utilizando los denominados tests de daños y de interés público: «Ambos, que pueden ser complementarios, consisten en realizar un balance entre el interés de retener la información y el interés de divulgarla para determinar si el beneficio público resultante de conocer la información solicitada es mayor que el daño que podría causar su revelación. El primero se centra en ponderar si la divulgación puede generar un daño presente, probable y específico a los intereses o valores protegidos de mayor entidad que los beneficios obtenidos; el segundo, en ponderar si el interés público a obtener con la entrega de la información justifica su divulgación y vence, con ello, la reserva» (Decisión C193-10). Así, por ejemplo, en la decisión Rol C664-10, relativa a las resoluciones recaídas en sumarios sanitarios donde aplicaba el derecho al olvido consagrado en el artículo 21 de la Ley N° 19.685, este Consejo resolvió dar acceso a dichas sanciones atendido el interés público involucrado en su conocimiento.

<sup>42</sup> Salvo, por cierto, que el CPLT en la resolución de un amparo al derecho de acceso a la información decida que esa información es pública. El punto es que en ese caso la información será pública para todos. Pero si el CPLT establece que la información es reservada entonces ésta automáticamente escapa del objeto del derecho de acceso a la información.

justicia, por mucho que ello riña con una de las garantías básicas de este derecho<sup>43</sup>.

Es cierto que una interpretación amplia del derecho de acceso a la información pública como vehículo idóneo para acceder a datos personales podría beneficiar a la ciudadanía. Pero también es cierto que esa postura está perpetuando una situación desfavorable para el derecho a la protección de datos personales, toda vez que los datos personales, como información reservada, deben ser interpretados en forma estricta y restrictiva y protegerlos sólo en la medida que no exista un interés público mayor que exija su revelación. El acceso a datos personales a través del derecho de acceso a la información- denominado habeas data impropio<sup>44</sup>- si bien soluciona un problema<sup>45</sup>, no explica por qué una misma información puede ser pública para unos pero reservada para otros, al tiempo que debilita la idea del control sobre los datos propios a través de un procedimiento cuyos principios no son coherentes con ese mandato.

---

43 Sobre esto véase Red Iberoamericana de Protección de Datos Personales "Viabilidad de Creación de Autoridades de Control en el Entorno Latinoamericano", en Huixquilucan (Estado de México), 4 de noviembre de 2005.

44 En el Habeas Data Impropio el objeto es acceder a información en poder del Estado, la cual puede contener datos personales.

45 Se refiere a la falta tanto de mecanismos expeditos para acceder a datos personales como de una autoridad de control que garantice el derecho.

## BIBLIOGRAFÍA

1. CASTILLO, Isabel- Cecilia (2007), *Protección de datos: Cuestiones constitucionales y administrativas* Thomson-Civitas, Madrid.
2. CERDA Silva, Alberto (2008), *Hacia un modelo integrado de regulación y control en la protección de datos personales*, Santiago.
3. CONTRERAS, Pablo y PAVÓN, Andrés (2012) *La Jurisprudencia del Consejo para la Transparencia sobre Acceso a la Información Pública y Seguridad de la Nación*, en *Ius et Praxis* (Vol. 18, No. 2), Santiago.
4. GUTIÉRREZ Castro, Rodrigo (2008) *Consideraciones y Recomendaciones en materia de tratamiento de datos personales por organismos públicos*, presentado en seminario técnico “Protección de datos personales”, organizado por Expansiva y la Facultad de Derecho de la Universidad de Chile, Santiago.
5. MARTÍNEZ Martínez, Ricard (2007) *El derecho fundamental a la protección de datos: perspectivas* En: «III Congreso Internet, Derecho y Política (IDP). Nuevas perspectivas» [monográfico en línea]. *Revista de Internet, Derecho y Política*. N.º 5. UOC.
6. RAJEVIC Mosler, Enrique (2010) *Protección de datos y transparencia en la administración pública chilena: inevitable y deseable ponderación* en el taller “Chile y la Protección de Datos Personales”, organizado por Expansiva, Santiago.
7. ROMERO Silvera, Graciela (2010) *Interés Público y Protección de Datos Personales, con especial referencia a los Derechos Humanos*; en Seminario Regional de Protección de Datos Montevideo, Uruguay.

8. QUEZADA Rodríguez, Flavio (2012) *La protección de datos personales en la jurisprudencia del Tribunal Constitucional de Chile*; Revista Chilena de Derecho y Tecnología. Vol., N° 1. Santiago.

Otras fuentes.

Fundación CEDDET y Agencia Española de Protección de Datos (2010) *El Derecho a la Protección de Datos Personales: Historia del derecho a la vida privada y el derecho a la protección de datos* 1ª Edición.

Red Iberoamericana de Protección de Datos Personales (2005) *Viabilidad de Creación de Autoridades de Control en el Entorno Latinoamericano* en Huixquilucan (Estado de México).

***Serie Bibliotecología y Gestión de Información.***

*Títulos publicados 2013*

N° 78 Internet, la Pedagogía y el síndrome de Robinson Crusoe. Álvaro Narea.

Disponible en : <http://eprints.rclis.org>

Alfredo Steinmeyer Espinosa

## NORMAS DE PUBLICACION

- **Objetivos**

La **Serie Bibliotecología y Gestión de Información** tiene por objetivo difundir la productividad, académica, las investigaciones y las experiencias de profesionales del área de la de Bibliotecología y Ciencia de la Información y del sector afin al mundo del libro y la lectura.

- **Alcance y política editorial**

Los trabajos a ser considerados en la Serie Bibliotecología y Gestión de Información, deben ser inéditos, no publicados en otras revistas o libros. Excepcionalmente el Comité Editorial podrá aceptar artículos que no cumplan con este requisito.

- **Arbitraje:** Los artículos recibidos serán sometidos a evaluación, a recomendación del Director de la Serie, donde el Comité Editorial enviará los trabajos a árbitros independientes para su aceptación o rechazo. En este último caso, se emitirá un informe al autor/a donde se señalen las razones de la decisión. El Comité Editorial podrá solicitar trabajos a autores de reconocido prestigio, quienes no serán sometidos al proceso de evaluación por árbitros.

- **Forma y preparación de manuscritos**

- **Extensión:** El artículo deberá tener una extensión entre 12 y 100 páginas, tamaño carta, espacio 1,5, cuerpo 12, incluidos gráficos, cuadros, diagramas, notas y referencias bibliográficas.
- **Idiomas:** Se aceptan trabajos en castellano, portugués e inglés, los cuales serán publicados en su idioma original.
- **Resumen y palabras claves:** El trabajo deberá tener un resumen en español e inglés en la primera página, de no más de 200 palabras, que sintetice sus propósitos y conclusiones más relevantes. De igual modo, deben incluirse tres palabras claves, que en lo posible no se encuentren en el título del trabajo, para efectos de indización bibliográfica.
- **Nota biográfica:** En la primera página, en nota al pie de página, deben consignarse una breve reseña curricular de los/as autores/as, considerando nacionalidad, título y/o grados académicos, desempeño y/o afiliación profesional actual y sus direcciones de correo electrónico, para posibles comunicaciones de los/las lectores/as con los autores/as.
- **Referencia bibliográfica:** Utilizar para las referencias bibliográficas la modalidad de (Autor, año) en el texto, evitando su utilización a pie de página. Ejemplo: (González, 2006). Agregar al final del texto, la bibliografía completa. Sólo con los/las autores/as y obras citadas, numeradas y ordenadas alfabéticamente. Para el formato de la bibliografía, utilizar la "Guía para la presentación de referencias bibliográficas de publicaciones impresas y electrónicas" disponible en formato electrónico en : <http://eprints.rclis.org/archive/00005163/01/ReferenciasBibliograficas.pdf>
- **Derechos:** Los derechos sobre los trabajos publicados, serán cedidos por los/as autores/as a la **Serie**.
- **Investigadores jóvenes:** El Comité Editorial considerará positivamente el envío de trabajos por parte de profesionales y/o investigadores/as jóvenes, como una forma de incentivo y apoyo a quienes comienzan su carrera en investigación.
- **Ejemplares de cortesía:** Los/as autores/as recibirán un ejemplar de cortesía del trabajo publicado.

- **Envío de manuscritos**

Todas las colaboraciones deberán ser enviadas impresas en duplicado. Los autores/as podrán remitir sus artículos en CD, o al correo electrónico: [hector.gomez@utem.cl](mailto:hector.gomez@utem.cl) , en programa Word (office).